Listing of Claims:

1. (Previously presented) A method for protection of computer assets from unauthorized access comprising:

receiving in a protection engine, an interface control command;

determining whether the interface control command introduces a security risk;

when the interface control command introduces a security risk, determining a state of a switch;

when the state of the switch is a protected state, inhibiting execution of the interface control command; and

when the state of the switch is an unprotected state, allowing execution of the interface control command.

2. (Previously presented) The method of claim 1 wherein inhibiting execution of the interface control command further includes:

providing an indication that the execution of the interface control command was inhibited.

3. (Previously presented) The method of claim 1 further comprising:

changing the state of the switch to the protected state when a timeout duration has elapsed.

4. (Previously presented) The method of claim 1 further comprising:

determining when the execution of the interface control command has been completed; and

when the execution of the interface control command has been completed, changing the state of the switch to the protected state.

5. (Previously presented) The method of claim 1 wherein determining the state of a switch includes:

determining the state of an electrical switch (physical switch).

6. (Previously presented) The method of claim 1 wherein determining the state of a switch includes:

determining the state of a software-based switch.

7. (Previously presented) The method of claim 6 wherein determining the state of the software-based switch includes:

using cryptographic techniques to determine the state of the software-based switch.

8. (Previously presented) The method of claim 1 wherein allowing execution of the interface control command further comprises:

allowing data to be written to a hard disk drive.

9. (Previously presented) The method of claim 8 wherein allowing data to be written to a hard disk drive comprises:

allowing data to be written to a boot sector of the hard disk drive.

10. (Previously presented) The method of claim 8 wherein allowing data to be written to a hard disk drive comprises:

allowing data to be written to a file allocation table of the hard disk drive.

11. (Previously presented) The method of claim 1 wherein allowing execution of the interface control command further comprises:

allowing data to be written to a floppy disk drive.

12. (Previously presented) The method of claim 1 wherein allowing execution of the interface control command further comprises:

allowing data to be written to a BIOS memory.

13. (Previously presented) The method of claim 1 wherein allowing execution of the interface control command further comprises:

allowing data to be written to a parallel port.

14. (Previously presented) The method of claim 1 wherein allowing execution of the interface control command further comprises:

allowing data to be written to a serial port.

15. (Previously presented) The method of claim 14 wherein allowing data to be written to a serial port further comprises:

allowing data to be written to a universal serial bus (USB).

16. (Previously presented) The method of claim 14 wherein allowing data to be written to a serial port further comprises:

allowing data to be written to an IEEE-1394 interface.

17. (Previously presented) The method of claim 13 wherein allowing execution of the interface control command further comprises:

allowing data to be written to a flash memory device.

18. (Previously presented) The method of claim 13 wherein allowing execution of the interface control command further comprises:

allowing data to be written to a thermal management controller.

19. (Previously presented) The method of claim 1 wherein determining whether the interface control command introduces a security risk comprises:

determining whether the interface control command is a hard disk drive formatting command.

20. (Previously presented) The method of claim 19 wherein determining whether the interface control command is the hard disk drive formatting command further comprises:

determining whether the interface control command is a boot sector write command.

21. (Previously presented) The method of claim 1 wherein determining whether the interface control command introduces a security risk comprises:

determining whether the interface control command is a program file write command.

22. (Previously presented) The method of claim 21 wherein determining whether the interface control command is a program file write command further comprises:

obtaining a file extension from the interface control command;

determining whether the file extension is an executable file extension.

23. (Previously presented) The method of claim 22 wherein determining whether the file extension is an executable file extension further comprises:

determining whether the file extension is one of an exe extension, a com extension, a bat extension, or a bin extension.

24. (Previously presented) The method of claim 1 wherein determining whether the interface control command introduces a security risk comprises:

determining whether the interface control command changes a file attribute, the file attribute enabling or disabling execution of a file corresponding to the file attribute.

25. (Previously presented) The method of claim 1 wherein determining whether the interface control command introduces a security risk comprises:

determining whether the interface control command disables a thermal management subsystem.

26. (Previously presented) The method of claim 25 wherein determining whether the interface control command disables a thermal management subsystem comprises:

determining whether the interface control command disables a fan.

27. (Previously presented) The method of claim 1 wherein determining whether the interface control command introduces a security risk comprises:

determining whether the interface control command is a write command to write to a system firmware (BIOS).

28. (Previously presented) The method of claim 1 wherein determining whether the interface control command introduces a security risk comprises:

determining whether the interface control command is a write command to write to a parallel port.

29. (Previously presented) The method of claim 1 wherein determining whether the interface control command introduces a security risk comprises:

determining whether the interface control command is a write command to write to a serial port.

30. (Previously presented) The method of claim 29 wherein determining whether the interface control command interface control command is a write command to write to a serial port comprises:

determining whether the interface control command is a write command to write to a universal serial bus (USB).

31. (Previously presented) The method of claim 29 wherein determining whether the interface control command is a write command to write to a serial port comprises:

determining whether the interface control command is a write command to write to an IEEE-1394 interface.

32. (Previously presented) The method of claim 1 wherein determining whether the interface control command introduces a security risk comprises:

determining whether the interface control command is a write command to write to a flash memory device.

33. (Previously presented) A method for protection of computer assets from unauthorized access comprising:

receiving in a protection engine in a south bridge, an interface control command;

determining whether the interface control command introduces a security risk;

when the interface control command introduces a security risk, determining whether a source of the interface control command is authentic;

when the source of the interface control command is not authentic, inhibiting execution of the interface control command; and

when the source of the interface control command is authentic, allowing execution of the interface control command.

34. (Previously presented) The method of claim 33 wherein inhibiting execution of the interface control command further includes:

providing an indication that the execution of the interface control command was inhibited.

35. (Previously presented) The method of claim 33 wherein allowing execution of the interface control command further comprises:

allowing data to be written to a hard disk drive.

36. (Previously presented) The method of claim 35 wherein allowing data to be written to a hard disk drive comprises:

allowing data to be written to a boot sector of the hard disk drive.

37. (Previously presented) The method of claim 35 wherein allowing data to be written to a hard disk drive comprises:

allowing data to be written to a file allocation table of the hard disk drive.

38. (Previously presented) The method of claim 33 wherein allowing execution of the interface control command further comprises:

allowing data to be written to a floppy disk drive.

39. (Previously presented) The method of claim 33 wherein allowing execution of the interface control command further comprises:

allowing data to be written to a BIOS memory.

40. (Previously presented) The method of claim 33 wherein allowing execution of the interface control command further comprises:

allowing data to be written to a parallel port.

41. (Previously presented) The method of claim 33 wherein allowing execution of the interface control command further comprises:

allowing data to be written to a serial port.

42. (Previously presented) The method of claim 41 wherein allowing data to be written to a serial port further comprises:

allowing data to be written to a universal serial bus (USB).

43. (Previously presented) The method of claim 41 wherein allowing data to be written to a serial port further comprises:

allowing data to be written to an IEEE-1394 interface.

44. (Previously presented) The method of claim 33 wherein allowing execution of the interface control command further comprises:

allowing data to be written to a flash memory device.

45. (Previously presented) The method of claim 33 wherein determining whether the interface control command introduces a security risk comprises:

determining whether the interface control command is a hard disk drive formatting command.

46. (Previously presented) The method of claim 45 wherein determining whether the interface control command is the hard disk drive formatting command further comprises:

determining whether the interface control command is a boot sector write command.

47. (Previously presented) The method of claim 33 wherein determining whether the interface control command introduces a security risk comprises:

determining whether the interface control command is a program file write command.

48. (Previously presented) The method of claim 47 wherein determining whether the interface control command is a program file write command further comprises:

obtaining a file extension from the interface control command;

determining whether the file extension is an executable file extension.

49. (Previously presented) The method of claim 48 wherein determining whether the file extension is an executable file extension further comprises:

determining whether the file extension is one of an exe extension, a com extension, a bat extension, or a bin extension.

50. (Previously presented) The method of claim 33 wherein determining whether the interface control command introduces a security risk comprises:

determining whether the interface control command changes a file attribute, the file attribute enabling or disabling execution of a file corresponding to the file attribute.

51. (Previously presented) The method of claim 33 wherein determining whether the interface control command introduces a security risk comprises:

determining whether the interface control command disables a thermal management subsystem.

52. (Previously presented) The method of claim 51 wherein determining whether the interface control command disables a thermal management subsystem comprises:

determining whether the interface control command disables a fan.

53. (Previously presented) The method of claim 33 wherein determining whether the interface control command introduces a security risk comprises:

determining whether the interface control command is a write command to write to system firmware (BIOS).

54. (Previously presented) The method of claim 33 wherein determining whether the interface control command introduces a security risk comprises:

determining whether the interface control command is a write command to write to a parallel port.

55. (Previously presented) The method of claim 33 wherein determining whether the interface control command introduces a security risk comprises:

determining whether the interface control command is a write command to write to a serial port.

56. (Previously presented) The method of claim 55 wherein determining whether the interface control command is a write command to write to a serial port comprises:

determining whether the interface control command is a write command to write to a universal serial bus (USB).

57. (Previously presented) The method of claim 55 wherein determining whether the interface control command is a write command to write to a serial port comprises:

determining whether the interface control command is a write command to write to an IEEE-1394 interface.

58. (Previously presented) The method of claim 33 wherein determining whether the interface control command introduces a security risk comprises:

determining whether the interface control command is a write command to write to a flash memory device.

59. (Previously presented) The method of claim 33 wherein determining whether the source of the interface control command is authentic comprises:

issuing a challenge to the source of the interface control command;

receiving a response from the source of the interface control command; and

determining whether the response is valid.

60. (Previously presented) The method of claim 59 wherein determining whether the response is valid comprises:

comparing the response to a mathematical function of a value accessible only to the protection engine and to an operating system.

61. (Previously presented) The method of claim 60 further comprising:

writing the value from a processor to a one-time-writable register in the protection engine (by an operating system) during a boot process (before application software is enabled).

62. (Previously presented) The method of claim 59 wherein determining whether the response is valid comprises:

performing a mathematical operation on the challenge to produce a correct response value; and

comparing the response to the correct response value.

63. (Previously presented) The method of claim 59 wherein issuing the challenge to the source of the interface control command includes:

obtaining a pseudorandom value; and

forming the challenge based on the pseudorandom value.

64. (Previously presented) Apparatus for protection of computer assets from unauthorized access comprising:

an interface controller operatively coupled to receive an interface control command to control an interface device;

a switch selectable between a protected state and an unprotected state;

a protection engine operatively coupled to the interface controller to receive the interface control command and operatively coupled to the switch to detect whether the switch is in the protected state or the unprotected state to determine whether the interface control command poses a security risk and to selectively inhibit or allow execution of the interface control command by the interface controller depending on whether or not the interface control command

poses the security risk and depending on whether the switch is in the protected state or the unprotected state.

65. (Original) The apparatus of claim 64 further comprising:

a timer operatively coupled to the switch to reset the switch to the protected state after a period of time has elapsed.

66. (Original) The apparatus of claim 64 further comprising:

an interface control command execution completion sensor operatively coupled to the switch to reset the switch to the protected state after an execution of the interface control command has been completed.

67. (Previously presented) Apparatus for protection of computer assets from unauthorized access comprising:

a south bridge comprising:

an interface controller operatively coupled to receive an interface control command to control an interface device; and

a protection engine operatively coupled to the interface controller for preventing unauthorized access to the interface device and operatively coupled to receive the interface control command to determine whether a source of the interface control command is authentic and to selectively allow or inhibit execution of the interface control command by the interface controller depending on whether or not the source of the interface control command is authentic.

68. (Original) The apparatus of claim 67 further comprising:

a one-time-writable register operatively coupled to the protection engine to store a value used to determine whether the source of the interface control command is authentic.

69. (Original) The apparatus of claim 68 wherein the value is accessible only to the protection engine and to an operating system.

70. (Previously presented) A method for protection of computer assets from unauthorized access comprising:

receiving in a protection engine, an interface control command;

determining whether the interface control command introduces a security risk determined from at least one of: a type of interface control command, an area of memory affected by the interface control command, a device affected by the interface control command, data associated with the interface control command, an operand associated with the interface control command, and a relationship of the interface control command to another interface control command;

when the interface control command introduces a security risk, determining a state of a switch;

when the state of the switch is a protected state, inhibiting execution of the interface control command; and

when the state of the switch is an unprotected state, allowing execution of the interface control command.

71. (Previously presented) The method of claim 70 including:

physically changing the state of a hardware switch by a user;

wherein determining the state of a switch includes determining the state of the hardware switch.

72. (Previously Presented) The method of claim 71 including performing at least one of: inhibiting data to be written to and allowing data to be written to a hard disk drive in response to determining the state of the hardware switch.

73. (Previously presented) The method of claim 70 including:

setting at least one bit in at least one of: a register and memory to change the state of a software-based switch; wherein determining the state of a switch includes:

determining the state of the software-based switch.